AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

SEC312-R2

Develop a strategy for automated remediation and response

Scott Ward (he/him)
Principal Solutions Architect,
External Security Services
AWS

Nicholas Jaeger (he/him)
Enterprise Solutions Architect
AWS

Things you should leave with

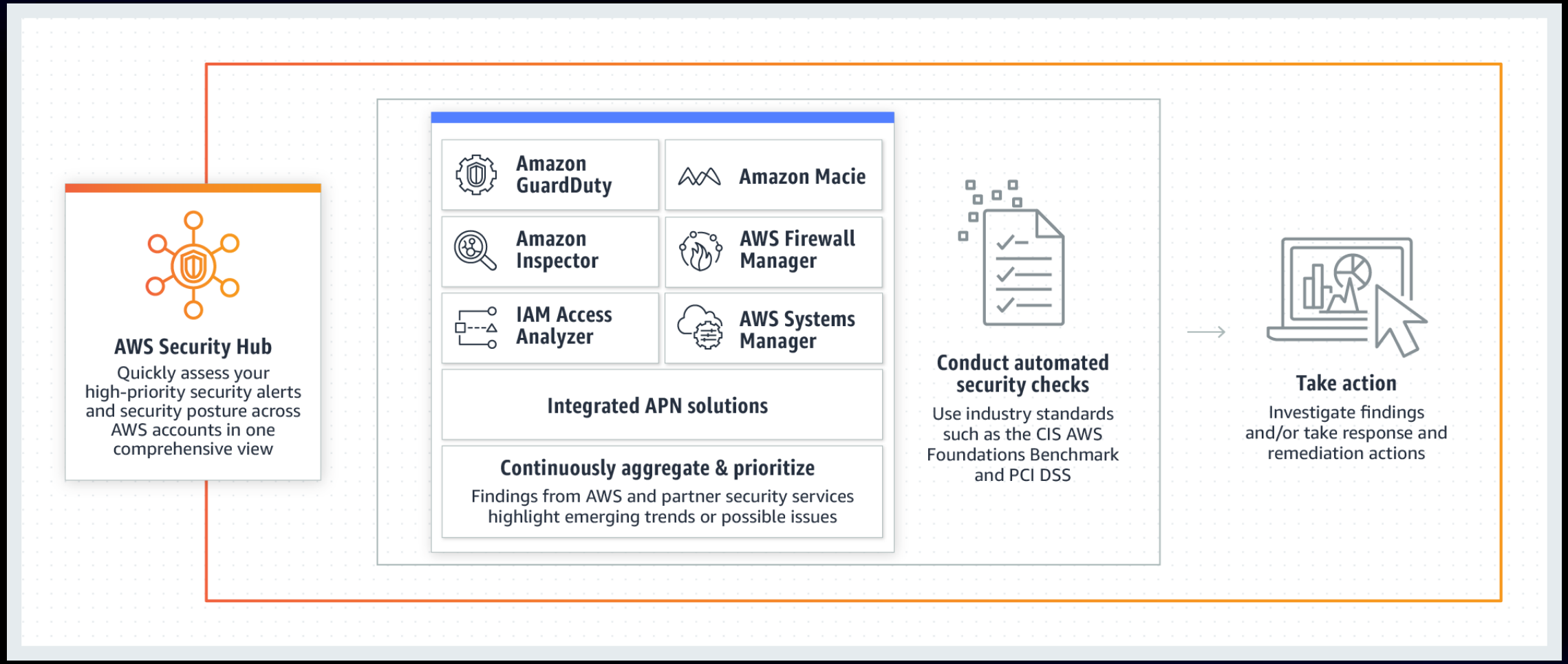
Use cases for AWS Security Hub

Integration flows with AWS Security Hub

Architecture approaches to enable response

Strategies on how to respond to security findings

What is AWS Security Hub?



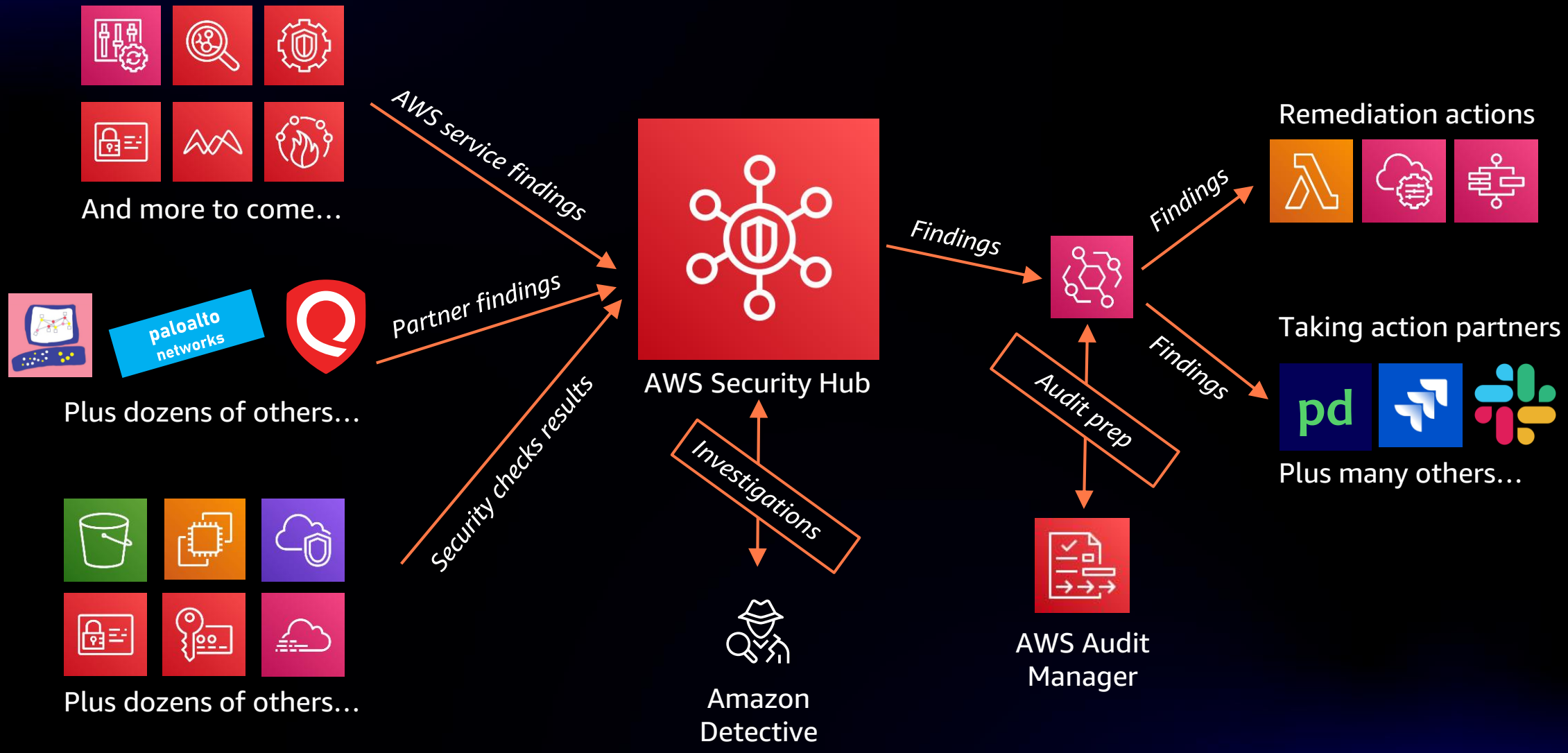
Use cases for AWS Security Hub

1) Centralized security and compliance

2) Centralized routing to a SIEM

3) Dashboard for account owners

AWS Security Hub information flows



Architecture

Responding to findings

Remediation strategy framework

	Destructive	Non-destructive
Prod	Cut ticket to resource or account owner	Auto-remediate
Non-Prod	Auto-remediate with delay or approval	Auto-remediate

Remediation and response scenarios

Scenario 1

Inspector generates findings for 20 instances all with critical CVEs.

Scenario 2

GuardDuty sends a finding that an API commonly used to collect data from an AWS environment was invoked in an anomalous way.

Scenario 3

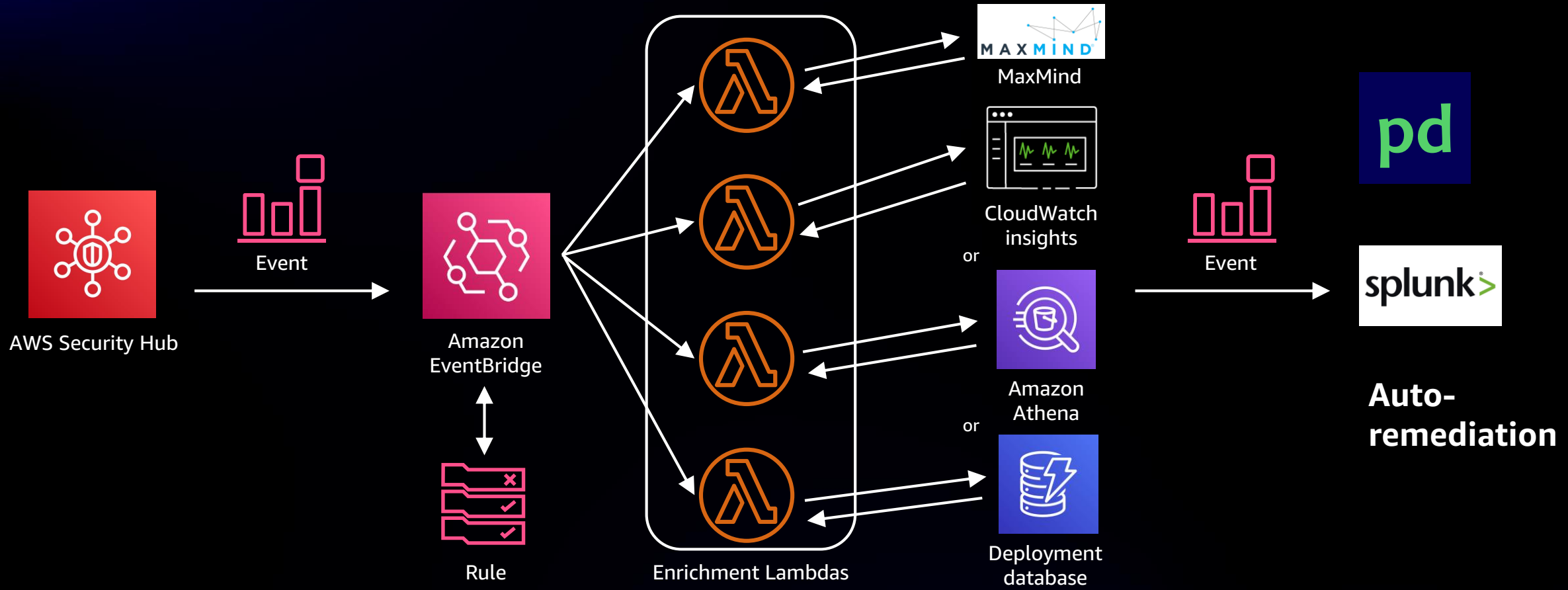
GuardDuty sends a finding that you have an EC2 instance that just started communicating with a known bad command and control server.

Scenario 4

Security Hub raises a best-practice finding that a bucket allows public access.

Examples

Example customer architecture (large FSI)



1. Security Hub finding automatically sent to EventBridge

2. EventBridge rules pick up relevant findings and trigger enrichment Lambdas

3. Finding is enriched with GeoIP data (MaxMind), contextual AWS CloudTrail data (insights), VPC flow, S3 access, ELB access logs (Athena), deployment/ business unit information (deployment database)

4. Enriched finding automatically sent to Amazon CloudWatch events

5. Tier 1/tier 2 findings are auto-remediated and archived, tier 3 findings are escalated

aws

Thank you!

Scott Ward

scotward@amazon.com

Nicholas Jaeger

jaegernj@amazon.com
linkedin.com/in/nickjaeger